SERVICE DESCRIPTION
FORTISANDBOX CLOUD

1. Introduction

With advanced threats rapidly increasing in number and sophistication, a perimeter firewall is just not enough. Customers need security that effectively detects unknown threats to complement next-generation firewalls and other security devices in their network. FortiSandbox™ Cloud service is an advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. Actionable intelligence generated by FortiSandbox Cloud is passed back into the network making it possible for preventive controls to disarm the threat.

FortiSandbox Cloud as a service offers an alternate deployment option to the FortiSandbox hardware appliance. It delivers the same rapid detection and automated response, but in the cloud. This provides unlimited flexibility to complement Fortinet appliances in any deployment scenario such as distributed enterprise, data center, and more.

The FortiSandbox Cloud service is available to purchase alongside the FortiGate/FortiWifi, FortiMail, FortiWeb and FortiProxy range of security appliances.

2. Service Features and Deliverables

The FortiSandbox Cloud service provides cloud based sandboxing capabilities for customers to be able to submit files for analysis from supported platforms. Following analysis the service will return appropriate intelligence back into the customer's environment to be actioned based on the customers security policy and configuration.

The service provides:

- Analysis of submissions with response provided back to customer infrastructure.
- Inspection of articles using Anti-Virus scanning, Cloud Query of recently discovered malware, Code Emulation, Virtual Sandbox and Call-Back detection. See FortiSandbox documentation for detailed description available at www.fortinet.com.
- Target analysis completion time of one hour average for all submissions over any twenty-four hour period.
- Management of Cloud infrastructure on a twenty four hours per day, seven days a week basis with target availability of 99.99%.

3. Customer Responsibilities

To ensure the full benefit of the service then the customer is required to provide the following:

- Create and manage a FortiCloud portal account at www.forticloud.com.
- Devices must be registered in the Customer Support Portal.
- Access the portal through supported web browser software with appropriate internet connectivity.
- Access to the internet with appropriate network access configuration enabling devices to communication with the service.
- Apply appropriate configuration of customer infrastructure to utilize the service including alignment with the customer security policy.
- Understanding and compliance with any relevant data protection laws or restrictions that governs the data contained within the submission to Fortinet.
- Ensure software levels on customer appliances are compliant with the service. Minimum levels include – FortiOS™ 5.2.3, FortiMail™ OS 5.3, FortiWeb™ 5.5.3, FortiADC™ 5.0, FortiProxy™1.0.
- Submit files for analysis only through supported protocols.
- Active and current Anti Virus, Anti Spam and virus outbreak licenses in use on appliances that interact with the service.

4. Submission Limits

To ensure the availability of the service for all customer, limits are applied to submissions based on device type and model contracted for the service. The limits are:

	Permitted Submissions	
	Per Minute	**Per Day**
FortiGate™		
FortiGate 30-90 / VM00	5	7200
FortiGate 100-400 / VM01	10	14400
FortiGate 500-900 / VM02 / VM04	20	28880
FortiGate 1000-2000 / VM08 / VM16	50	72000
FortiGate 3000 / VM32 (and higher models)	100	144000
FortiWeb		
FortiWeb 100/VM01	5	7200
FortiWeb 400 / VM02	10	14400
FortiWeb 600-1000 / VM04	20	28880
FortiWeb 2000 / VM08	40	57600
FortiWeb 3000	70	100800
FortiWeb 4000	100	144000
FortiADC		
FortiADC 60 / VM01	5	7200
FortiADC 100-400 / VM02	10	14400
FortiADC 700 / VM04	20	28880
FortiADC 1000-2000 / VM08	50	72000
FortiADC 4000	100	144000
FortiProxy		
FortiProxy 400E	20	28880
FortiProxy 2000E	100	144000
FortiProxy 4000E	200	288800
FortiProxy VM	100	144000

	File Submissions		URL Submissions	
	Per Minute	**Per Day**	**Per Minute**	**Per Day**
FortiMail				
FortiMail 60x / VM00	5	7200	1	1440
FortiMail 200 / VM01	10	14400	2	2880
FortiMail 400 / VM02	20	28800	4	5760
FortiMail 900 / 1000 / VM04	40	57600	8	11520
FortiMail 2000 / VM08	70	100800	14	20160
FortiMail 3000 / VM16 (and higher models)	100	144000	20	28800

5. Scope & Conditions

- This service is covered by the (then up to date), current Fortinet Service Terms and Conditions located at https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf.
- An active FortiCare™ 8x5 or 24x7 contract is a requirement for activation of the service on the Fortinet Hardware.
- Objects will be retained within the platform for the duration of analysis before being discarded. Any item not scanned within a 2 hours from submission will also be discarded. Any item not accepted into the processing queue within 1 hour will also be discarded.
- Logging of suspicious or malicious activity will be retained for a period of one year before being deleted permanently.
- Fortinet will make a determination of analysis queue priority based on the type of appliance submitting to the service and may make adjustment to this as appropriate to ensure an optimized customer experience.
- File submission limits are applicable based on appliance type and model. The service targets apply to submissions within those limits with all exceptions only being processed if service capacity exists.

- In the event that continued provision of the service to the customer would compromise the integrity or security of the service, the customer agrees that Fortinet may temporarily limit or suspend the Service to the customer.
- Customer agrees to use the service for legitimate and lawful business purposes only. Should Fortinet discover illegal activity, or activity likely to undermine the integrity of the service, regardless of intent, the service may be terminated without notice and where appropriate the relevant authorities notified.
- Any loss of connectivity by the customer that is not as a result of failure of Fortinet managed infrastructure, is the responsibility of the customer with the service continuing to be considered as being utilized. Availability targets only apply to the FortiCloud infrastructure.
- Planned maintenance and upgrade may need to be carried out which could impact the availability of FortiSandbox Cloud Services. When such maintenance activity is required, Fortinet will aim to avoid any service disruption. In any event, Fortinet will endeavor to limit impact to the availability of FortiSandbox Cloud Services to maximum window of eight hours in single calendar month and to provide the customer with forty eight hours advanced notice. Notification will be made through the most appropriate method dependent on user impacted and which may include email, portal messages or other means.
- On the rare occasion that the integrity of the cloud service is at risk then Fortinet may be required to perform emergency maintenance actions. In this instance Fortinet will target to inform all affected parties within one hour of the start of the maintenance activity.
- The service will be delivered in accordance with Fortinet's privacy policy made available and updated from time to time at https://www.fortinet.com/corporate/about-us/privacy.html. Usage of FortiCloud implies that the Customer and not Fortinet are potentially exporting the data submitted. The customer is responsible for ensuring that their use of FortiCloud services is in accordance with any applicable laws or regulations.

6. Eligibility & Purchasing

The service is available for purchase by an enterprise customer or end-user through authorized Fortinet resellers and distributors globally. The service is delivered to the customer or end-user of Fortinet products as referenced in the purchase order placed with Fortinet by a customer or Fortinet authorized partner or distributor.

The duration of the service is three hundred and sixty five days from activation per purchased service unit. The service may be cancelled by the end-user at any time and for any reason, but in no event will Fortinet refund any prepaid subscription fee. All sales are final.

Purchasing Information:

FortiSandbox Cloud Service	FC-10-xxxxx-123-02-12

Where XXXXX is defined by the appliance or platform it may apply to. Please refer to your price list to identify the specific SKU for the appropriate Product.